(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
21 November 2002 (21.11.2002)

PCT

(10) International Publication Number
WO 02/093838 A1

(51) International Patent Classification[7]: H04L 12/26, 12/56, H04M 3/22

(21) International Application Number: PCT/EP01/05583

(22) International Filing Date: 16 May 2001 (16.05.2001)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant (for all designated States except US): NOKIA CORPORATION [FI/FI]; Keilalahdentie 4, FIN-02150 Espoo (FI).

(72) Inventors; and
(75) Inventors/Applicants (for US only): SEURUJÄRVI, Jorma [FI/FI]; Tampereentie 414 B9, FIN-33880 Lempäälä (FI). KALLIO, Seppo [FI/FI]; Maijalankatu 9 As 13, FIN-33720 Tampere (FI). MARTIN, Markus [FI/FI]; Puistokaari 6 A 8, FIN-Helsinki 00200 (FI). MARTTI, Lumme [FI/FI]; c/o Nokia Corporation, Keilalahdentie 5, FIN-02150 Espoo (FI).

(74) Agents: PELLMANN, Hans-Bernd et al.; Tiedtke-Bühling-Kinne et al., Bavariaring 4, 80336 München (DE).

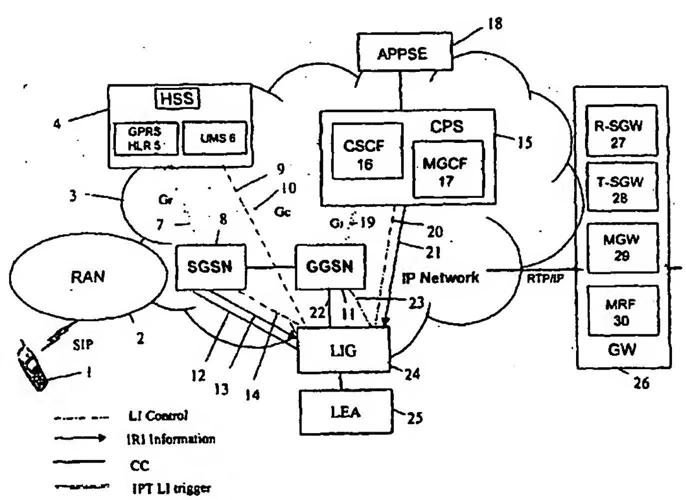
(81) Designated States (national): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States (regional): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— with international search report

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: METHOD AND SYSTEM ALLOWING LAWFUL INTERCEPTION OF CONNECTIONS SUCH A VOICE-OVER-INTERNET-PROTOCOL CALLS



(57) Abstract: The invention relates to a method and communication system allowing interception of a communication or connection of a target to be intercepted. According to preferred embodiments of the invention, interception triggering information is transmitted between the user plane and control plane (e.g. via Gr-, Gc-, Gi-interfaces).The system comprises at least one control means for handling signalling of a connection between a user equipment and another communication device, and a support element for transmitting traffic information between the user equipment and the another communication device. When the connection is to be intercepted, the control means is adapted to generate an interception information for informing the support element or another network element on an identification of the target to be intercepted. The support element is adapted to copy the traffic information to another network element for interception when receiving an interception information from the control means.

WO 02/093838 A1

TITLE

METHOD AND SYSTEM ALLOWING LAWFUL INTERCEPTION OF CONNECTIONS SUCH AS VOICE-OVER-INTERNET-PROTOCOL CALLS

DESCRIPTION

FIELD AND BACKGROUND OF THE INVENTION

The invention relates to a method and system enabling interception of traffic between network elements, in particular in a case where the traffic is transported based on protocols adapted for internet-involving connections such as IP (Internet Protocol) or other type of packet-based protocols.

Fig. 12 shows a diagram of a system for lawful interception (LI) on the GPRS (General Packet Radio Service) plane. Apart from the elements 24, 25, 42, the network structure and network elements are in accordance with known standards or proposals.

In this application LIGs contain Administration Function (ADMF), Delivery Function 2 (DF2) and Delivery Function 3 (DF3), or as in Fig. 7 DF3 is integrated to network elements.

A network element 1, e.g. a terminal equipment TE and/or a mobile terminal MT of a subscriber, is connectable to the mobile network via a radio access network 2 which, according to Fig. 11, is implemented as a UMTS radio access network (UTRAN) but may also be a radio access network of other type. The system further comprises a home subscriber server (HSS) 4, one or more serving support nodes (SGSN, Serving GPRS Support Node) 8, one or more gateway nodes (GGSN, Gateway GPRS Support Node) 11, one or more call state control

functions (CSCF) 16, one or more media gateway control functions (MGCF) 17, and cooperates with, or includes one or more network elements 18 for providing applications and services (APPSE). The network element 18 includes one or more service control points (SCP).

The system further comprises SGWs 28 (Transport Signalling Gateway), MGWs (Media Gateways) 29, MRF (Multimedia Resource Function) 30 and provides connections to other networks such as PSTN (Public Switched Telephone Network), legacy/external network 41, a virtual private network (VPN 42), multimedia IP networks 43 and legacy signalling network 44, etc.

As shown in Fig. 11, for performing lawful interception (LI), a Lawful Interception Gateway (LIG) 24 is provided which may be connected to or cooperate with a Law Enforcement Agency (LEA) 25 and may be connected to the support nodes 8 and/or 11 for intercepting traffic between a network element to be intercepted (e.g. network element) and another called or calling terminal. The elements involved in lawful interception are marked by hatched lines. In Fig. 11, the dual line represents "control, call related information and call content". The broken line represents signalling connections. The continuous single line represents "signalling and data transfer".

The system shown in Fig. 12 is able to intercept GPRS-based normal communications. However, a problem arises when interception is to be conducted with an internet-protocol-type connection such as a VoIP (Voice over IP) connection. GGSNs 11 normally do not recognise VoIP subscribers with IPT (IP telephony) identity. GPRS interception can therefore presently only be used for GPRS connections but not for VoIP connections.

In particular when the intended lawful interception (LI) does

not relate to the user identity on the transport level (i.e. the ID's used by GPRS) but only to user identities used in the IM (Internet Multimedia) subsystem which are only known to the CSCF 16 (e.g. firstname.surname@sip.someoperator.com.), the support nodes 8 and/or 11 do not have information for identifying the call and call contents to be intercepted.

As an example, if the voice calls of a subscriber are to be intercepted, the GPRS support nodes may not be able to identify the calls by only relying on the PDP (Packet Data Protocol) contexts.

SUMMARY OF THE INVENTION

The invention provides a method and/or system with enhanced possibility of intercepting connections such as calls which are based on protocols adapted for internet or similar type.

The present invention provides a method and/or system as defined in the independent claims or any of the dependent claims.

In accordance with a preferred embodiment of the invention, a control means such as CSCF is adapted to trigger an interception and has the necessary call-related information to identify the connections to be intercepted. The control element informs one or more of the support nodes such as SGSN or GGSN which PDP contexts should be intercepted. As an example, typically the call-related information should be reproduced or copied in a voice call interception will be interpreted in the control element while it is just another PDP context on the GPRS level. Therefore, an interaction between the control element and a support node is provides so that an interception can also be performed in a case where

the interception does not relate to the user identity on the transport level but only to the identity used on other levels such as in the IM subsystem. The control element thus is able to inform the support nodes such as GGSN to monitor VoIP subscriber's call contents.

Otherwise stated, according to preferred embodiments, it is the application which runs on top of the services provided by the GPRS layer which will be intercepted and not every application used by the subscriber to be intercepted.

According to some of the preferred embodiments interception triggering information is transmitted between the user plane and control plane (e.g. via Gr-, Gc-, Gi-interfaces).

As a general concept, a control element such as CSCF or HSS informs one or more support network elements such as GGSN or SGSN to start sending user plane data to an intercept structure, e.g. a LIG.

The control means is able to inform a support node such as GGSN to monitor the subscriber's call content, e.g. of a VoIP call, in a standardised way.

The proposed solution offers the control means such as CSCF a standardised possibility to intercept VoIP call content using the existing GPRS solution implemented in GGSN. Gi interface may be a standardised interface.

The invention introduces several alternatives of call interception in an All-IP (Internet Protocol) environment.

In one of the solutions, call content is intercepted from GGSN and call related information (reports) from CSCF and/or from application servers. The call control signaling may be put through SGSN and GGSN in one PDP context, and CSCF is the

first to recognize that the subscriber is to be monitored. CSCF is able to inform GGSN to copy the actual media, i.e. user traffic (both directions if needed) also to interception equipment, in addition to forwarding the actual media to the called terminal's address, in particular IP address.

The invention may e.g. be used in an IP concept involving CPS and GGSN.

The solution proposed according to the invention is advantageous over a theoretical alternative way of sending the triggering information via the LEA which would otherwise be required if the core network (SGSN and/or GGSN) and the control plane (CPS and HSS) are of different type, e.g. from different producers. The proposed solution is a faster way to trigger the interception.

In accordance with an implementation of the invention, the LI in an All-IP Network (interception of VoIP 'calls' etc.) may be triggered in HSS and in CPS by setting appropriate triggers or trigger detection points in these elements.

The interception is preferably triggered from the IPT Identity. The IPT Identity may e.g. be: IMSI, alias (e.g. user_id@domain_id), E.164 number (MSISDN), or IP address.

When the user plane does not have knowledge about alias, it can at least provide triggering to other identities used in the user plane.

The IRIs (Intercept Related Information) from the control plane and CC (Content of Communication) from the user plane have to be bound together, i.e. correlated. In the embodiments shown in the drawings, Interception ID is preferably used as correlation ID.

Another possible correlation ID can be the call-related ID for charging purposes. This ID will be used in control and user plane.

In further embodiments, the triggering information is assumed to be available in Gr and Gc interfaces, because HSS can get alias-related IMSI, MSISDN, PDP context, IP address and maybe IMEI.

The triggering information is preferably provided also in Gi interface e.g. in case of terminated or forwarded party being a target for interception, when the SCP (Service Control Point) has only the subscriber's alias and MSISDN information.

If the charging ID cannot be used as a correlation information, the correlation ID should be delivered to the SGSN and GGSN with a LI trigger (in Gr, Gc and Gi interfaces).

The delivery of the CC content to the LEA is preferably performed in accordance with standards and national laws (separation of directions, in speech or in data packets, etc.).

If the used codec information is not available in the SGSN or in the GGSN, CPS preferably delivers it to the LIG.

If the context contains packets from several "calls", SGSN, GGSNor LIG preferably filters off packets not to be intercepted.

Control and IRI interfaces between LIG - CPS and between LIG - HSS are preferably provided.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 illustrates a first embodiment of the invention,

Fig. 2 illustrates a second embodiment of the present invention,

Fig. 3 illustrates a third embodiment of the present invention,

Fig. 4 illustrates a fourth embodiment of the present invention,

Fig. 5 illustrates a fifth embodiment of the present invention,

Fig. 6 illustrates a sixth embodiment of the present invention,

Fig. 7 illustrates a seventh embodiment of the present invention,

Fig. 8 illustrates an eighth embodiment of the present invention,

Fig. 9 illustrates a ninth embodiment of the present invention,

Fig. 10 illustrates a tenth embodiment of the present invention,

Fig. 11 illustrates another embodiment of the present invention, and

Fig. 12 illustrates a structure for lawful interception in a

pure GPRS-based system according to the prior art.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS OF THE INVENTION

The drawings illustrate LI scenarios with GPRS access. In case of other access (e.g. WLAN), the LI or at least copying the CC from the access is adapted accordingly.

In a preferred embodiment, for LI, in particular VoIP interception, the LI trigger is transmitted from HSS and CPS at least when the used identity is alias or other IPT identity which is not in user plane knowledge.

In Gi interface, the intercepted subscriber MSISDN or IP address is used to identify the intercepted context. Interception equipments (LEAs) IP address may also be used depending on the solution. CSCF may use the Gi interface to control VoIP interception in GGSN.

This invention presents at least three different implementations how the interception is carried out after the information about the IP address is passed over the Gi interface.

1) GGSN picks up an IP address of LEA (Law Enforcement Agency) from CSCF over the Gi interface and sends copies of all data packets also to that address. Signalling traffic is sent from CSCF to LIG (Lawful Interception Gateway)which then forwards them to LEA.

2) GGSN picks up an IP address of IF over the Gi and copies all data packet there. LIG then forwards data packets via MGW (Media GateWay) to LEA. Signaling traffic is similar as in case 1.

3) This is similar to case 2, but there the data traffic is sent directly from LIG to LEA, not via MGW.

The problem may also be solved without CSCF and GGSN communicating. In this case, the CSCF may forward the IP address to LIG, which then handles the interception similar to known GPRS-based Interception.

As a basic information to the embodiments shown in Figs. 1 to 9, HSS has knowledge about subscriber's all IPT identities but CPS has only knowledge about subscriber's alias and MSISDN.

Fig. 1 shows a first embodiment of a method and system in accordance with the present invention. The same reference numerals as in Fig. 12 have been assigned to network elements similar to the network elements shown in Fig. 12 and described above. A mobile terminal 1 can get access and be attached to a network 3, preferably an IP network, via a radio access network RAN 2 which may correspond to UTRAN of Fig. 12 or be based on a GPRS standard, etc. The network 3 comprises one or more serving support nodes 8 (SGSN = Serving GPRS Support Node) and one or mode gateway support nodes 11 (GGSN = Gateway GPRS Support Node). A home subscriber server HSS 4 includes a home location register (HLR) 5 and a user mobility server (UMS) 6.

A call processing server (CPS) 15 of network 3 comprises a call state control function (CSCF) 16 and a media gateway control function (MGCF) 17 and is adapted to cooperate with the applications and services component (APPSE) 18. The network 3 communicates with other networks or components (not shown) via a gateway 26 using an internet protocol such as RTP (Real Time Protocol). The gateway 26 includes a roaming signalling gateway function (R-SGW) 27, a transport

signalling gateway function (T-SGW) 28, a media gateway (MGW) 29, and a multimedia resource function (MRF) 30. Further, the structure shown in Fig. 1 includes a lawful interception gateway (LIG) 24 which is adapted to communicate with a law enforcement agency (LEA) 25.

The structure shown in Fig. 1 allows a legal interception of IP-based connections between a user equipment such as mobile terminal 1 and another terminal equipment, e.g. of a called or a calling party. According to the structure of Fig. 1, standardised interfaces Gr, Gc, Gi may be used, in particular when all components necessary for interception are provided by the same supplier or producer.

In the embodiment shown in Fig. 1, the double-dotted lines 7, 11, 19 illustrate connections for providing and transmitting trigger information for triggering the interception in case of an IP telephony (IPT) or other type of connection to be intercepted. The trigger information will be sent to SGSN 8 and/or GGSN 11 when an interception is to be started. The trigger information will be sent from HSS 4 to SGSN 8 via interface Gr and link 7, and/or to GGSN 11 via interface Gc and link 10, and/or from CPS 15 to GGSN 11 via interface Gi and link 19.

The dot-and-dash lines 9, 14, 20 and 23 shown between HSS 4, SGSN 8, CPS 15 and GGSN 19, respectively, on the one hand, and LIG 24, on the other hand, illustrate the interception control, i.e. transmission of the control information, control commands and the like necessary for lawful interception control. The solid lines 12 and 22 shown between SGSN 8 and GGSN 11, on the one hand, and LIG 24 on the other hand represent CC (Content of Communication) which is sent to LIG 24 for interception. The arrow-headed lines 13, 21 illustrate the flow of IRIs (intercept-related information).

In case the interception is handled by SGSN 8 alone without involving GGSN 11, the links / connections 22, 23 between GGSN 11 and LIG 24 can be omitted. Vice-versa in case the interception is handled by GGSN 11 alone, links and information flows 12 to 14 between SGSN 8 and LIG 24 can be omitted. For enhancing quality and success rate of interception, all links / information flows shown in Fig. 1 may also be provided in parallel between SGSN 8 and GGSN 11 on the one hand, and LIG 24, on the other hand.

In the embodiment shown in Fig. 1, the triggering information is available in Gr and Gc interfaces and is provided by HSS 4 which gets alias-related IMSI, MSISDN, PDP context, IP address and/or possibly IMEI.

In Fig. 1, the triggering information may preferably also be provided in the Gi interface, in particular in a case when a terminated or forwarded party is the interception target.

Stated more generally, in the solution according to Fig. 1, the control and user planes are composed of elements of the same producer, and all Gr, Gc and Gi interfaces are standardised interfaces. In more detail, HSS 4, CPS 15, SGSN 8, GGSN 11 and LIG 24 are from the same producer and are in the same VPN (Virtual Private Network).

LIG 24 controls triggers (i.e. delivers IPT identities activation information) in the HSS 4 and in the CPS 15. HSS 4 will trigger the interception from the IPT identity. HSS 4 can set the LI trigger for all IPT identities but at least the alias triggering is needed. HSS 4 will map the triggered IPT ID to such a format (IMSI [default], MSISDN, IMEI or IP address) that LIG 24 or SGSN 8 or GGSN 11 will recognize it. HSS 4 will send the mapped LI trigger and correlation ID (if charging ID is not enough to bind IRIs and CC together) to the SGSN 8 and/or GGSN 11 directly (via Gr, Gc).

If Gr, Gc and Gi interfaces are used, the trigger and possible correlation information is preferably standardised to those interfaces. If it is necessary to carry IPT identity (and PDP context ID) or the mapped LI trigger and correlation ID (if charging ID is not enough to bind IRIs and CC together) from HSS 4 to SGSN 8 and GGSN 11 via Gr and Gc and from CPS 15 to GGSN 11 via Gi for other reason than interception (e.g. charging or statistic) those interfaces can be standardised. With those Gr, Gc and Gi standards the IPT identity or mapped LI trigger can be used as a LI triggering key in SGSN and GGSN.

SGSN 8 and/or GGSN 11 will send the CC (containing also correlation ID, charging ID or other correlation ID) to the LIG 24. SGSN 8 and CPS 15 wil send IRI information to the LIG 24.

Some IPT identities are in CPS knowledge (alias and MSISDN) so CPS 15 can trigger the LI and send the trigger key to the GGSN 11 e.g. in case a terminated or forwarded party is a target for interception. CPS 15 will send all communication related IRI information (containing also correlation information) to the LIG 24. IRI information can be sent to the LIG also from the HSS if it is needed. Such a information can be e.g. location information if it is not known in SGSN 8 or CPS 15.

LIG 24 will create the reports for LEA and will separate user medias from the CC if it is requested by the authority or standards.

Fig. 2 illustrates a further embodiment of the invention. In this and all further embodiments shown in Figs. 3 to 9 the same reference numerals are assigned to components having the

same or essentially the same structure or functioning as the components shown in Figs. 1 or 12. All above explanations regarding these components, their functioning and possible alternatives likewise apply to the components shown in Figs. 2 to 9 (unless otherwise stated below) and are therefore not repeated again.

The embodiment shown in Fig. 2 differs from the embodiment of Fig. 1 in that no standardised interfaces Gr, Gc, Gi between HSS 4 and SGSN 8, GGSN 11, and between CPS 15 and GGSN 11 are provided or used for interception. According to Fig. 2 the trigger information (information flow 10) is sent from HSS 4 directly to LIG 24 instead to GGSN and SGSN 8 (as shown in Fig. 1).

Likewise, the trigger information (information flow or link 19) is directly sent from CPS 15 to LIG 24 (instead to GGSN 11 as in Fig. 1). The other information flows or connections 9, 12 to 14, and 20 to 23 are similar to the embodiment of Fig. 1. That is, the interception control (dot-and-dash lines 9, 14, 20, and 23), the IRI information flow (lines 13, 21), and the CC flow (lines 12, 22) are the same as in Fig. 1.

In this embodiment, the LIG 24 informs the SGSN 8 and/or GGSN 11 on the address or other identification of the party or equipment to be intercepted.

In the embodiment of Fig 2, the control and user planes (HSS, CPS, SGSN, GGSN and LIG) are composed of elements of the same producer, and both Gr and Gc are non-standardised interfaces. HSS, CPS, SGSN, GGSN and LIG are in the same VPN.

LIG 24 controls triggers in the HSS 4 and in the CPS 15 (delivers IPT identities activation information to these elements). HSS 4 will trigger the interception from the IPT identity. HSS can provide the trigger for all IPT identities

but at least the alias triggering is necessary. HSS 4 will map the triggered IPT ID to a format (IMSI [default], MSISDN, IMEI or IP address) that LIG or SGSN or GGSN can recognize. HSS will send the mapped LI trigger (e.g. IMSI) and correlation ID (if charging ID is not enough to bind IRIs and CC together) to the SGSN and/or GGSN via LIG.

If Gr, Gc and Gi standards do not support IPT identity and/or mapped LI trigger and/or possible correlation ID, the LI 24 is triggered via LIG 24, in particular in a case when standards are against delivering LI information in open interfaces (e.g. in USA). In such a case HSS 4 and CPS 15 will send the mapped LI trigger and correlation ID (if charging ID is not enough to bind IRIs and CC together) to the LIG 24. LIG 24 will send the LI trigger immediately to the SGSN 8 and/or GGSN 11.

SGSN or/and GGSN will send the CC (containing also correlation ID, charging ID or other correlation ID) to the LIG. SGSN, CPS and possible HSS will send IRI information to the LIG.

Some IPT identities are known to CPS 15 (alias and MSISDN) so it can trigger the LI and send the trigger key to the GGSN e.g. in case of terminated or forwarded party being a target for interception. CPS will send all communication related IRI information (containing also correlation information) to the LIG. IRI information can be sent to the LIG also from the HSS if it is needed. Such an information can be e.g. location information if it not known in SGSN 8 or CPS 15.

LIG will create the reports for LEA and will separate user medias from the CC if it is requested by the authority or standards.

One of the advantages of Fig. 2 is the fact that no standardised interfaces or other communication between HSS 4, SGSN 8, GGSN 11, and CPS 15 are necessary for starting, controlling and performing interception.

Fig. 3 shows a further embodiment in accordance with the present invention which includes, in addition to the components of the embodiment shown in Fig. 1, an additional lawful interception gateway (LIG) 31 which is adapted to communicate with LEA 25, similar to LIG 24. The embodiment according to Fig. 3 allows a VoIP LI with control of LI by LIG 24, and actual performing of the LI by LIG 31. According to the embodiment of Fig. 3, the identification information (IRI information) is sent to LIG 24 from HSS 4 (information flow or link 32), and from CPS 15 (information flow or link 21). In addition, similar to the embodiment of Fig. 1, the LI control information (lines 9, 20) is sent from HSS 4 and CPS 15 to LIG 24. The CC information is directly sent to LIG 31 from SGSN 8 and/or GGSN 11 (lines 12, 22). According to Fig. 3, the IRI information is directly sent from SGSN 8 to LIG 31 to inform the latter on the address or other identification of the party or equipment to be intercepted.

The embodiment of Fig. 3 is of advantage in that it enables a distinction between LI control and actual interception of communication content. The LIG 31 may be a gateway of any type which must simply be able to communicate with SGSN 8 and/or GGSN 11 but does not require to communicate, or be able to communicate, with HSS 4 and/or CPS 15. For instance, different LIG components 24, 31 produced by different producers may be used. As in Fig. 1, the structure of Fig. 3 preferably provides standardised interfaces Gr, Gc, Gi for allowing a proper communication between HSS 4, SGSN 8, GGSN 11 and CPS 15.

In the scenario according to Fig. 3, IPT identity or LI

trigger (and PDP context ID) and possible correlation ID are carried from HSS to SGSN and GGSN via Gr and Gc interface, and from CPS to GGSN via Gi also in other cases than interception (e.g. charging or statistic). The carrying manner may be standardised. IPT identity or LI trigger (e.g. IMSI) can be used as a LI triggering key in SGSN 8 and GGSN 11. Note that the trigger in the Gi interface can be only the alias or MSISDN (only they are known to CPS 15).

HSS 4, CPS 15 and LIG 24 are preferably from the same producer or supplier, and LIG 31 is from a different producer or supplier. HSS 4, CPS 15 and LIG 24 are in the same VPN.

Here is assumed that Charging ID can be used as a correlation information with user identity (e.g. IPT identity). Otherwise also correlation ID is preferably standardised to the Gr, Gc and Gi interfaces.

LIG controls triggers in the HSS 4 and in the CPS 15 (deliver IPT identities activation information). IRI information can be sent to the LIG also from the HSS if it is needed. Such a information can be e.g. location information if it is not in CPS's knowledge.

HSS will trigger the interception from the IPT identity. HSS can make the LI trigger (e.g. IMSI) from all IPT identities but at least the trigger from alias (user@domain) is needed. HSS will send the LI trigger to the SGSN and GGSN directly (Gr, Gc). CPS will trigger the interception e.g. in case of terminated or forwarded party being a target for interception and will send trigger key (alias or MSISDN) to the GGSN.

One supplier may produce IRIs from the control plane (HSS and CPS) and the other supplier may produce LI trigger related (trigger in Gr and Gc) CC and possible IRIs to the LEA.

The embodiment of Fig. 4 essentially represents a combination of the embodiments of Figs. 2 and 3 and does not require any standardised interfaces between HSS 4, SGSN 8, GGSN 11 and CPS 15. The additional LIG 31 and the LIG 24 operate in the same manner as shown and described with regard to Fig. 3 and receive the same information as in the embodiment of Fig. 3.

In this embodiment of Fig. 4, Gr and Gc interfaces have non-standardised IPT ID or LI trigger correlation ID information.

HSS 4, CPS 15 and LIG 24 are from one vendor and are in the same VPN.

Here, the Charging ID or other standardised ID which is used in both control and user plane is used as a correlation ID with user identity (e.g. IPT identity or IMSI).

LIG 24 controls triggers in the HSS 4 and in the CPS 15 (deliver IPT identities activation information). IRI information can be sent to the LIG 24 also from the HSS 4 if it is needed. Such an information can be e.g. location information if unknown by CPS 15.

HSS 4 and CPS 15 will trigger the interception from the IPT identity. HSS 4 and CPS 15 will send IRIs containing IPT identity or LI trigger and correlation ID (and PDP context) to the LIG 24.

IRIs will be produced from the control plane (HSS and CPS). The CC and possible IRIs will be produced and transmitted from SGSN and/or GGSN to the LEA, and will only be related to other IPT identities (IMSI, MSISDN and IP address) than alias.

In Fig. 5, the gateways 24, 31 are exchanged as compared to the arrangement of Fig. 4. According to Fig. 5, an additional LI control flow or link 33 is provided between GGSN 11 and LIG 24. Moreover, standardised interfaces Gr, Gc, Gi are provided, similar to Fig. 1, between HSS 4, SGSN 8, GGSN 11 and CPS 15.

According to Fig. 5, IPT identity (and PDP context ID) and possible correlation ID are carried from HSS to SGSN and GGSN via Gr and Gc interfaces and from CPS to the GGSN via Gi interface for other reason than interception (e.g. charging or statistic) and in a standardized manner. IPT identity can be used as a LI triggering key in SGSN and GGSN.

SGSN 8, GGSN 11 and LIG 24 are in the same VPN.

Here, Charging ID is used as a correlation information with user identity (e.g. IPT identity). Other correlation information is preferably standardised to the Gr and Gc interfaces.

LIG 24 controls triggers (IPT identity) in the SGSN and in the GGSN. If Gr, Gc and Gi will support only the trigger mapped from the IPT identity e.g. IMSI, SGSN 8 and GGSN 11 cannot start interception related to alias (user@domain). Preferably, also SGSN 8 and GGSN 11 know IPT identities, because it is possible that neither the LEA 25 nor the LIG 24 know the alias correspondence.

HSS will trigger the interception from the IPT identity. HSS can make the LI trigger represented by any needed identity (IMSI, E.164, IP address, IMEI and IPT identity). In this scenario, the Gr and Gc interfaces are informed on the IPT identity itself.

IRIs and CC will be produced from the user plane (SGSN and

GGSN) and IRIs will be produced from the control plane.

To ensure the reliability of the interception in a case where SGSN and GGSN cannot reliably start the interception related to IPT identity, IPT identity is set and known in HSS 4, CPS 15, SGSN 8, GGSN 11 and LIG 24, 31, because the target can communicate with other user's UE (User Equipment) by using his own alias (user@domain).

Fig. 6 illustrates an embodiment having a similar structure as the embodiments of Figs. 4 and 5, but without the need of standardised interfaces Gr, Gc, Gi. An additional IRI information link 35 is provided between HSS 4 and LIG 31. Further, a control link 34 is present between SGSN 8 and LIG 24. Such a link is already provided in the embodiment of Fig. 5.

The structure of Fig. 6 provides VoIP LI with a core network made of components of e.g. the same producer, as well as an additional LIG 31 which may be provided by another producer. Non-standardised interfaces may be provided without problems because of the shown information flows.

According to this embodiment, Gr and Gc interfaces have non-standardised IPT ID (nor PDP context) information.

SGSN 8, GGSN 11 and LIG 24 are in the same VPN.

Here, the Charging ID is used as a correlation information with user identity (e.g. IPT identity, at least in control plane LI).

CC and IRIs will be produced from the user plane (SGSN and GGSN) and IRIs will be produced from the control plane. CC and IRIs can be produced from the SGSN and GGSN related to other IPT identity (IMSI, MSISDN and IP address) than alias.

Figs. 7 to 9 illustrate three further embodiments which are structurally based on the configuration of components shown in Fig. 12. Components shown in Fig. 12 and not represented in the embodiments of Figs. 7 to 9 (e.g. components 4, 18, 43, 44) are preferably likewise provided in the embodiments according to Figs. 7 to 9 and are simply omitted for sake of clarity. In the structure shown in Fig. 12, only signalling information can be reported. Contrary thereto, in accordance with the embodiments shown in Figs. 7 to 9 three alternatives of VoIP interception are shown which use the Gi interface between CSCF 16 and GGSN 11 (and/or SGSN 8).

In the embodiment shown in Fig. 7, the alias or MSISDN of the target to be intercepted is used to identify the context to be intercepted. The target alias or MSISDN is preferably sent from CSCF 16 to GGSN 11 via the Gi interface. It is also possible to deliver the IP address of the other party communicating with the party to be intercepted, and/or the IP address of LEA 24 from CSCF 16 to GGSN 11 via the Gi interface. This information flow is shown in Fig. 7 as well as in Figs. 8 and 9 by a dot-and-dash line referenced 51 in Fig. 7. Therefore, GGSN 11 can pick the alias or MSISDN of the interception target, and eventually also the IP address of the other party communicating with the target, and/or of LEA 24 from the Gi interface. The CSCF 16 further communicates, in all embodiments shown in Figs. 7 to 9, with a lawful interception gateway 50 via an information flow, link or channel 52 which transmits control and call related information. The LIG 50 may be provided in a virtual private network (VPN) 42 and may transmit and/or receive control and call-related information to and from LEA 24 via an information flow channel, link, etc. 55. These features likewise apply to the embodiments shown in Figs. 8 and 9.

According to the embodiment of Fig. 7, the IP call content

represented by double-broken lines 53, 54, 56 is transmitted from GGSN 11 to LEA 24 via media gateway 29 and PSTN/legacy/external network 41. Both directions of information flow between the target and the other party may be separated and separately copied and transmitted to LEA 24.

In Figs. 7 to 9, the signalling flow is represented by a single dot-and-dash line whereas signalling and data transfer is represented by single solid lines.

Fig. 8 illustrates a further embodiment having essentially the same structural arrangement as the embodiment of Fig. 7. In the embodiment of Fig. 8, the GGSN 11 is adapted to send the VoIP content directly to the LIG 50. The LIG 50 separates both directions from the VoIP media streams it receives from GGSN 11 and sends them separately to the media gateway 29 for further transmission to the other party communicating with the target to be intercepted and for copying it to LEA 24 (via information flow link 56). The information flow between GGSN 11, LIG 50 and MGW 29 is represented by double-broken lines 60, 61. Similar to the embodiment of Fig. 7, the target IP address is used to identify the intercepted context in the embodiment of Figs. 8 and 9.

Fig. 9 illustrates a further embodiment having a structure similar to the structures of the embodiments of Figs. 7 and 8. According to Fig. 9, the GGSN 11 is sending the VoIP content to the LIG 50 as represented by link or channel 60. The LIG 50 separates both directions from the VoIP media stream it receives from GGSN 11 and sends them separately to the LEA 24, as represented by information flow 70. The GGSN 11 may send the VoIP content to the other party communicating with the target to be intercepted in the customary manner, e.g. via MGW 29.

According to the embodiments shown in Figs. 8 and 9, the GGSN

11 may receive the IP address of LIG 50 from the Gi interface to CSCF 16.

Fig. 10 illustrates a further embodiment of the present invention. In this embodiment, only the LIG 24 of the Control plane vendor is needed. To ensure CC content delivery to the LIG IPT identity or LI trigger (and PDP context ID), the delivery address (or addresses) of the LIG 24 and possible correlation ID are carried from HSS 4 to SGSN 8 and GGSN 11 via Gr and Gc, and from CPS 15 to GGSN 11 via Gi interface. Note that the trigger in the Gi interface can be only the alias or MSISDN (only they are known to the CPS 15).

HSS 4, CPS 15 and LIG 24 preferably are from the same vendor so as to ensure good compatibility, and are in the same VPN.

The Charging ID may be used as a correlation information with user identity (e.g. IPT identity). Otherwise also correlation ID may be standardised to the Gr, Gc and Gi interfaces. Also delivery address(es) of the LIG 24 is preferably standardised to the interfaces.

LIG 24 controls triggers in the HSS 4 and in the CPS 15 (i.e. delivers IPT identities activation information and LIG's delivery addresses). IRI information can be sent to the LIG 24 also from the HSS 4 if it is needed. Such an information can be e.g. location information if it is not known in CPS 15.

HSS 4 will trigger the interception from the IPT identity. HSS 4 can generate the LI trigger (e.g. IMSI) from all IPT identities but at least the trigger from alias (user@domain) is needed. HSS 4 will send the LI trigger to the SGSN 8 and GGSN 11 directly (via Gr, Gc). CPS 15 will trigger the interception e.g. in case of terminated or forwarded party

being a target for interception and will send trigger key (alias or MSISDN) to the GGSN 11.

IRIs are produced from the control plane (HSS and CPS). LI trigger related (trigger in Gr, Gc and Gi) CC will be delivered to the LIG 24.

Fig. 11 shows another embodiment of the present invention.

This embodiment illustrates some methods to ease the implementation and to provide more throughput to the Lawful Interception.

A problem in VoIP is not only the data collection but also the interpretation of the collected data. When VoIP call goes through GPRS or any other data network it can be captured normally using IMSI, IMEI or MSISDN as target. This embodiment uses e.g. a standard data collection and introduces several different interpretation methods.

In VoIP lawful interception the voice is digital and transmitted in packets. Combining these packets stream to listenable audio stream needs special software and hardware.

This problem might be solved by providing a new element that converts the intercepted voice packet streams to circuit switched (CS) data streams. These CS data streams could then be routed to LEA (lawful enforcement authorities).

In accordance with the present embodiment of the invention, the interpretation and storing of the VoIP interception product is transferred to LEAs. Advantages of the implementation in accordance with the present embodiment include the reduction of the amount of needed network elements. Further, the throughput of the delivery is better because there is no interpretation or format change for the

intercepted product.

The decoding back to voice occurs at LEA site with the machines thereof and using their capacity. The load is this way also distributed to the users.

The LEAs can play back and forth the intercepted content with an appropriate program such as Windows Multimedia Player just as easy as with a normal tape recorder.

The solution uses existing systems so that no new machines are needed. No switched circuit capacity problems occur at delivery interfaces. No unnecessary encoding/decoding takes place in the network.

In the following, some alternative solutions are presented:

The data is collected and processed to known voice file formats (e.g. wav, mp3, au) at LIB (Lawful interception Browser, DF2 in ETSI terminology) or at LEAs machine. Normally the LEAs machine is a personal computer that contains www browser which has means of playing the standard audio files. The police authority (LEA) may then study this intercepted data just by playing the files and listening to the voice from computers speakers.

As an alternative, the data is processed to real audio stream and delivered in realtime to the listening sites. The person or equipment at LEA may the connect to these stream and listen to the intercepted VoIP call.

In an alternative solution, the data exists already in coded compact format which can be transformed to audible form by a special new plug-in module for the browsers. This alternative introduces a new audio data format for the browsers but uses as much as possible the already coded VoIP data.

The embodiment shown in Fig. 11 comprises a user equipment 40 which may be similar to element 1 and conducts a call to be intercepted. The call is connected through a GSM or UMTS network 41 and further through a GPRS network 42 which may be an IP-based network. The signalling and user traffic of the call is handled by a SGSN 8 and an GGSN 11, similar to the above described embodiments.

The network 42 includes a LIC (Lawful Interception Controller) 43 and a LIB (Lawful Interception Browser) 44. An authorised person or equipment such as a jugde instructs the LIC 43 to perform LI of calls/connections of the user of equipment 40. The LIC 43 sends instructions and information to the LIB 44 for intercepting the traffic, i.e. the call content of connections of the equipment 40. The LIB 44 sends the detected call content packets to the LEA 25 which interprets the packets for transforming them into audible form.

Whereas the embodiments of Figs. 1 to 10 are mainly directed to the manner of implementing the interception of VoIP on the system level, that means from where the intercepted content is collected, the embodiment of Fig. 11 is mainly directed to the processing of CC (CommunicationContent) data by collecting or listening with browser. The voice information is not passed to the LEA in analog form. In practise the advantage of this invention is that a digital internet based application format may be used so that for LEA users it is easy to find programs. One of the advantages of this invention is that it makes coding/decoding easier, and actually transfers coding to LEA.

The functioning and/or structure of the embodiment of Fig. 11 as shown and described above, can be integrated into, or combined with, any of the embodiments of Figs. 1 to 10.

Although the invention has been described above with reference to specific embodiments, the invention intends to cover other embodiments as well which represent combinations of the above features, omissions, amendments, alternatives etc.

CLAIMS

1. Communication system comprising at least one control means for handling signalling of a connection between a user equipment and another communication device, and a support element for transmitting traffic information between the user equipment and the another communication device, wherein, when the connection is to be intercepted, the control means is adapted to generate an interception information for informing the support element or another network element on an identification of the connection to be intercepted, and the support element is adapted to copy the traffic information to another network element for interception.

2. Communication system according to claim 1 wherein the control means is a CPS (Call Processing Server) or CSCF (Call State Control Function).

3. Communication system according to any one of the preceding claims, wherein the support element is a Serving Support Node and/or a Gateway Support Node.

4. Communication system according to any one of the preceding claims, wherein the support element is a Serving GPRS Support Node (SGSN) and/or Gateway GPRS Support Node (GGSN).

5. Communication system according to any one of the preceding claims, comprising an interface between the support element and the control means for transmitting the interception information.

6. Communication system according to claim 5, wherein the interface is a Gi, Gc or Gr interface.

7. Communication system according to any one of the preceding claims, wherein the interception information transmitted to the support element indicates an address, preferably an IP address, of the target (party or equipment) to be intercepted.

8. Communication system according to any one of the preceding claims, wherein the interception information transmitted to the support element indicates an address, preferably an IP address, of the other party connected to the target to be intercepted.

9. Communication system according to any one of the preceding claims, wherein the interception information transmitted to the support element indicates an address, preferably an IP address, of a Law Enforcement Agency (LEA) or Law Enforcement Monitoring Function (LEMF), the support element being adapted to send copies of data traffic to and/or from the target to be intercepted to the indicated address.

10. Communication system according to claim 9, wherein the support element is adapted to send copies of the data traffic to a Media Gateway for forwarding the traffic to the Law Enforcement Agency (LEA) or Law Enforcement Monitoring Function (LEMF).

11. Communication system according to any one of the preceding claims, wherein the interception information transmitted to the support element indicates an address, preferably an IP address, of a Lawful Interception Gateway (LIG), the support element being adapted to send copies of

data traffic to and/or from the target to be intercepted to the indicated address.

12. Communication system according to claim 11, wherein the Lawful Interception Gateway is adapted to directly send the copies of the data traffic to a Law Enforcement Agency (LEA) or Law Enforcement Monitoring Function (LEMF).

13. Communication system according to claim 11, wherein the Lawful Interception Gateway is adapted to send the copies of the data traffic to a Media Gateway for forwarding the traffic to a Law Enforcement Agency (LEA) or Law Enforcement Monitoring Function (LEMF).

14. Communication system according to claim 11, 12, or 13, wherein the Lawful Interception Gateway is adapted to separate both directions of the media to and from the target to be intercepted and to forward them separately to a Media Gateway or Law Enforcement Agency (LEA) or Law Enforcement Monitoring Function (LEMF).

15. Communication system according to any one of the preceding claims, wherein the support node is adapted to separate both directions of the media to and from the target to be intercepted and to forward them separately to a Media Gateway or Law Enforcement Agency (LEA) or Law Enforcement Monitoring Function (LEMF).

16. Communication system according to any one of the preceding claims, wherein the control means is adapted to send signalling traffic, related to the connection to and/or from the target to be intercepted, to a Lawful Interception Gateway (LIG).

17. Communication system according to claim 16, wherein the Lawful Interception Gateway (LIG) is adapted to forward

the received signalling traffic to a Law Enforcement Agency (LEA) or Law Enforcement Monitoring Function (LEMF).

18. Communication system according to any one of the preceding claims, wherein the connection to be intercepted is a VoIP (Voice over IP) media connection.

19. Communication system according to any one of the preceding claims, wherein an authorised interception agency, e.g. Law Enforcement Agency (LEA), is adapted for interpretation and storing of the intercepted traffic information content.

20. Communication system according to any one of the preceding claims, wherein the data is collected and processed to a voice file format at a LIB (Lawful interception Browser, DF2 in ETSI terminology) or at a machine of LEA.

21. Communication system according to any one of the preceding claims, wherein the data is processed to audio stream, e.g real audio, and delivered in realtime to a monitoring site.

22. Communication system according to any one of the preceding claims, wherein the data exists in coded compact format and is transformed to audible form by a browser module.

23. Method to be performed in a communication system comprising at least one control means for handling signalling of a connection between a user equipment and another communication device, and a support element for transmitting traffic information between the user equipment and the another communication device, wherein, when the connection is to be intercepted, the control means generates an interception information for informing the support element or

another network element on an identification of the connection to be intercepted, and the support element copies the traffic information to another network element for interception when receiving an interception information.

24. Method according to claim 23, wherein the control means is a CPS (Call Processing Server) or CSCF (Call State Control Function).

25. Method according to claim 23 or 24, wherein the support element is a Serving Support Node and/or a Gateway Support Node.

26. Method according to any one of the preceding method claims, wherein the support element is a Serving GPRS Support Node (SGSN) and/or Gateway GPRS Support Node (GGSN).

27. Method according to any one of the preceding method claims, comprising an interface between the support element and the control means for transmitting the interception information.

28. Method according to claim 27, wherein the interface is a Gi, Gc or Gr interface.

29. Method according to any one of the preceding method claims, wherein the interception information transmitted to the support element indicates an address, preferably an IP address, of the target (party or equipment) to be intercepted.

30. Method according to any one of the preceding method claims, wherein the interception information transmitted to the support element indicates an address, preferably an IP address, of the other party connected to the target to be intercepted.

31. Method according to any one of the preceding method claims, wherein the interception information transmitted to the support element indicates an address, preferably an IP address, of a Law Enforcement Agency (LEA) or Law Enforcement Monitoring Function (LEMF), the support element being adapted to send copies of data traffic to and/or from the target to be intercepted to the indicated address.

32. Method according to claim 31, wherein the support element sends copies of the data traffic to a Media Gateway for forwarding the traffic to the Law Enforcement Agency (LEA) or Law Enforcement Monitoring Function (LEMF).

33. Method according to any one of the preceding method claims, wherein the interception information transmitted to the support element indicates an address, preferably an IP address, of a Lawful Interception Gateway (LIG), the support element being adapted to send copies of data traffic to and/or from the target to be intercepted to the indicated address.

34. Method according to claim 33, wherein the Lawful Interception Gateway is adapted to directly send the copies of the data traffic to a Law Enforcement Agency (LEA) or Law Enforcement Monitoring Function (LEMF).

35. Method according to claim 33, wherein the Lawful Interception Gateway is adapted to send the copies of the data traffic to a Media Gateway for forwarding the traffic to a Law Enforcement Agency (LEA) or Law Enforcement Monitoring Function (LEMF).

36. Method according to claim 33, 34, or 35, wherein the Lawful Interception Gateway is adapted to separate both directions of the media to and from the target to be

intercepted and to forward them separately to a Media Gateway or Law Enforcement Agency (LEA) or Law Enforcement Monitoring Function (LEMF).

37. Method according to any one of the preceding method claims, wherein the support node is adapted to separate both directions of the media to and from the target to be intercepted and to forward them separately to a Media Gateway or Law Enforcement Agency (LEA) or Law Enforcement Monitoring Function (LEMF).

38. Method according to any one of the preceding method claims, wherein the control means sends signalling traffic, related to the connection to and/or from the target to be intercepted, to a Lawful Interception Gateway (LIG).

39. Method according to claim 38, wherein the Lawful Interception Gateway (LIG) is adapted to forward the received signalling traffic to a Law Enforcement Agency (LEA) or Law Enforcement Monitoring Function (LEMF).

40. Method according to any one of the preceding method claims, wherein the connection to be intercepted is a VoIP (Voice over IP) media connection.

41. Method according to any one of the preceding method claims, wherein an authorised interception agency, e.g. Law Enforcement Agency (LEA), performs interpretation and storing of the intercepted traffic information content.

42. Method according to any one of the preceding method claims, wherein the data is collected and processed to a voice file format at a LIB (Lawful interception Browser, DF2 in ETSI terminology) or at a machine of LEA.

43. Method according to any one of the preceding method

claims, wherein the data is processed to audio stream, e.g. real audio, and delivered in realtime to a monitoring site.

44. Method according to any one of the preceding method claims, wherein the data exists in coded compact format and is transformed to audible form by a browser module.

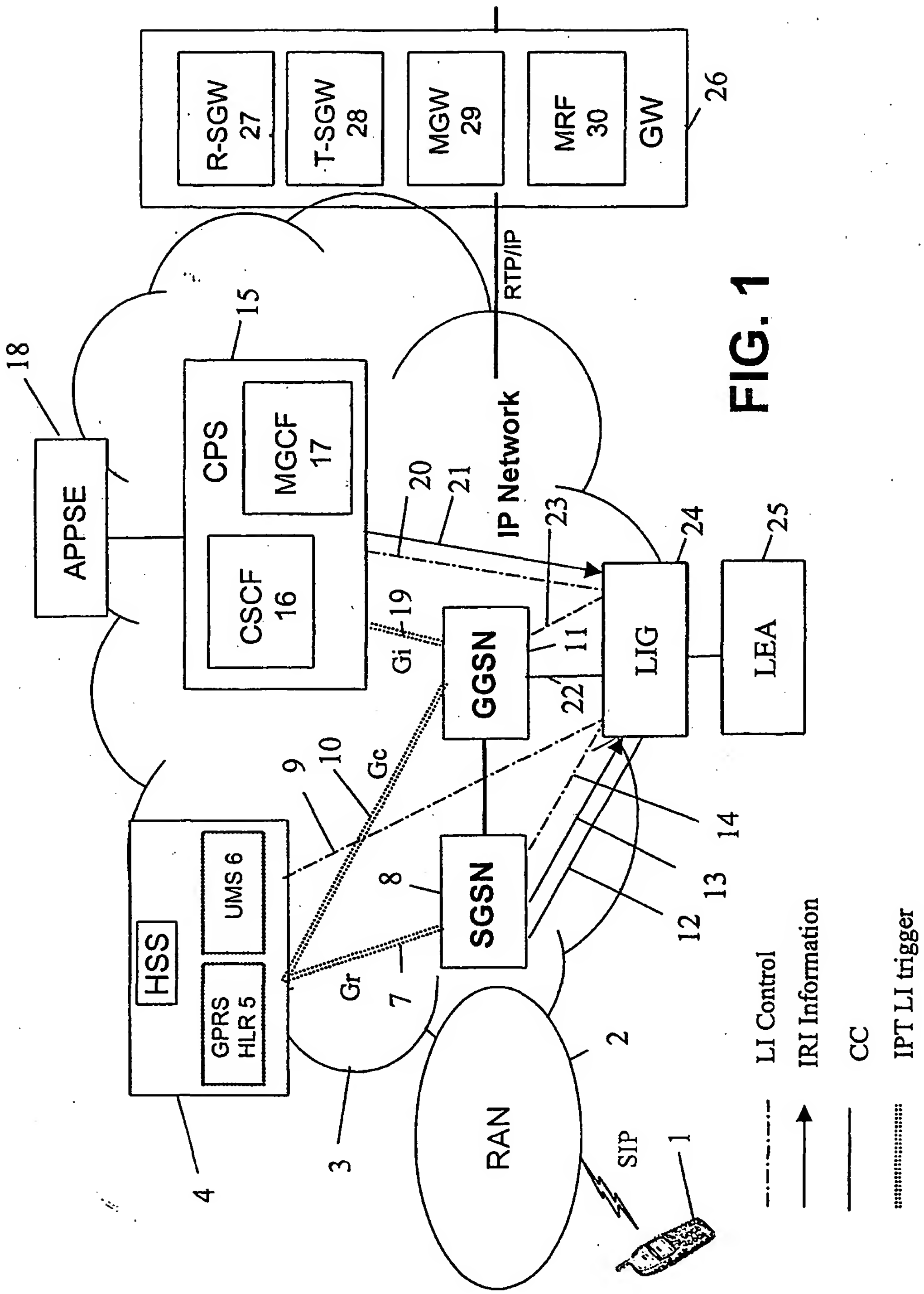

R-SGW 27
T-SGW 28
MGW 29
MRF 30
GW
26
RTP/IP
15
18
APPSE
CPS
MGCF 17
CSCF 16
20
21
IP Network
23
24
25
LIG
LEA
19
Gi
GGSN
11
22
9
10
Gc
HSS
UMS 6
GPRS HLR 5
8
SGSN
Gr
7
14
13
12
2
RAN
SIP
1
3
4
LI Control
IRI Information
CC
IPT LI trigger

FIG. 1

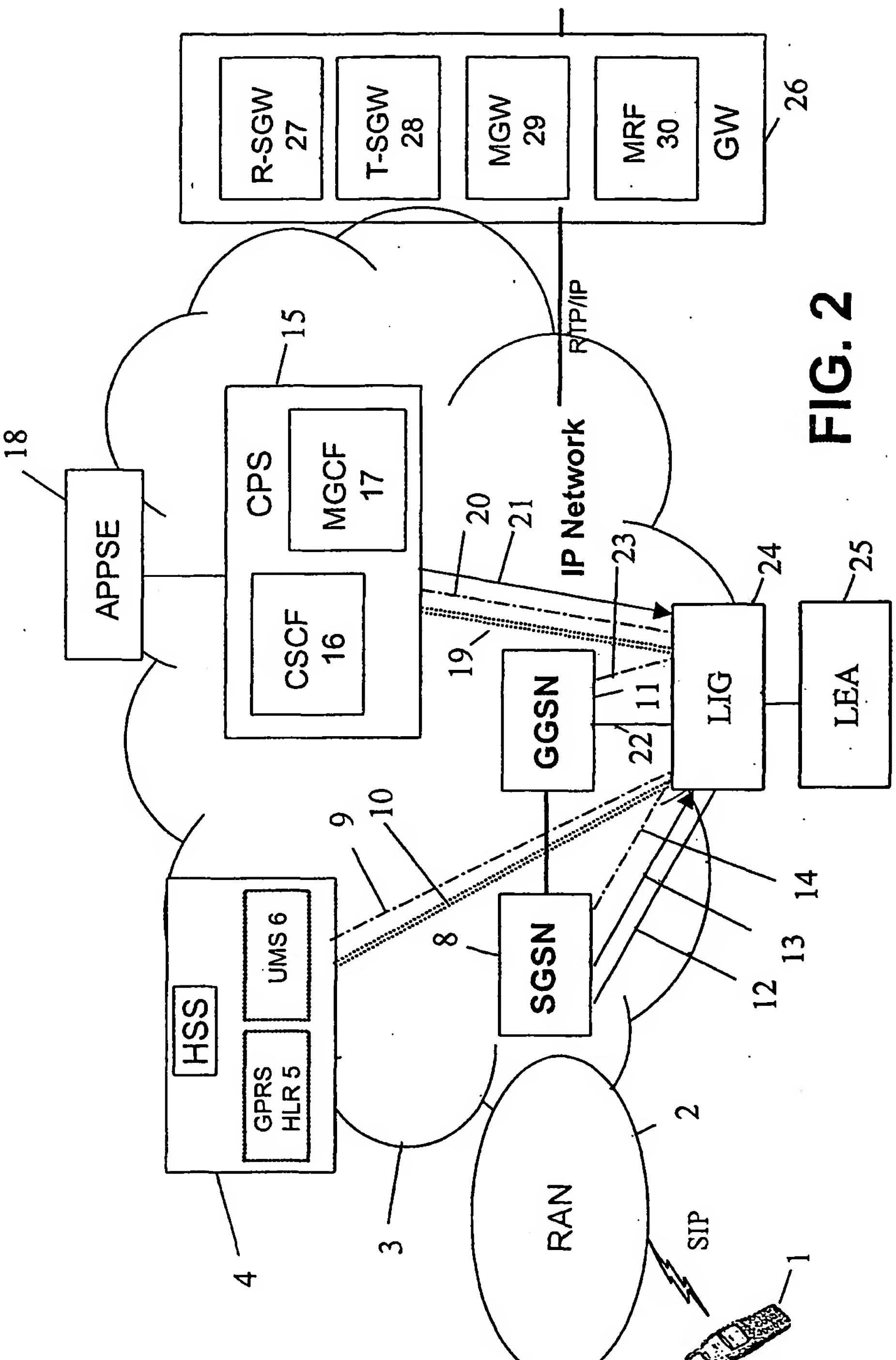

R-SGW 27
T-SGW 28
MGW 29
MRF 30
GW
26
RTP/IP
IP Network
15
CPS
MGCF 17
CSCF 16
18
APPSE
20
21
23
24
25
19
GGSN
11
22
LIG
LEA
9
10
8
HSS
UMS 6
GPRS HLR 5
SGSN
14
13
12
4
3
2
RAN
SIP
1

FIG. 2

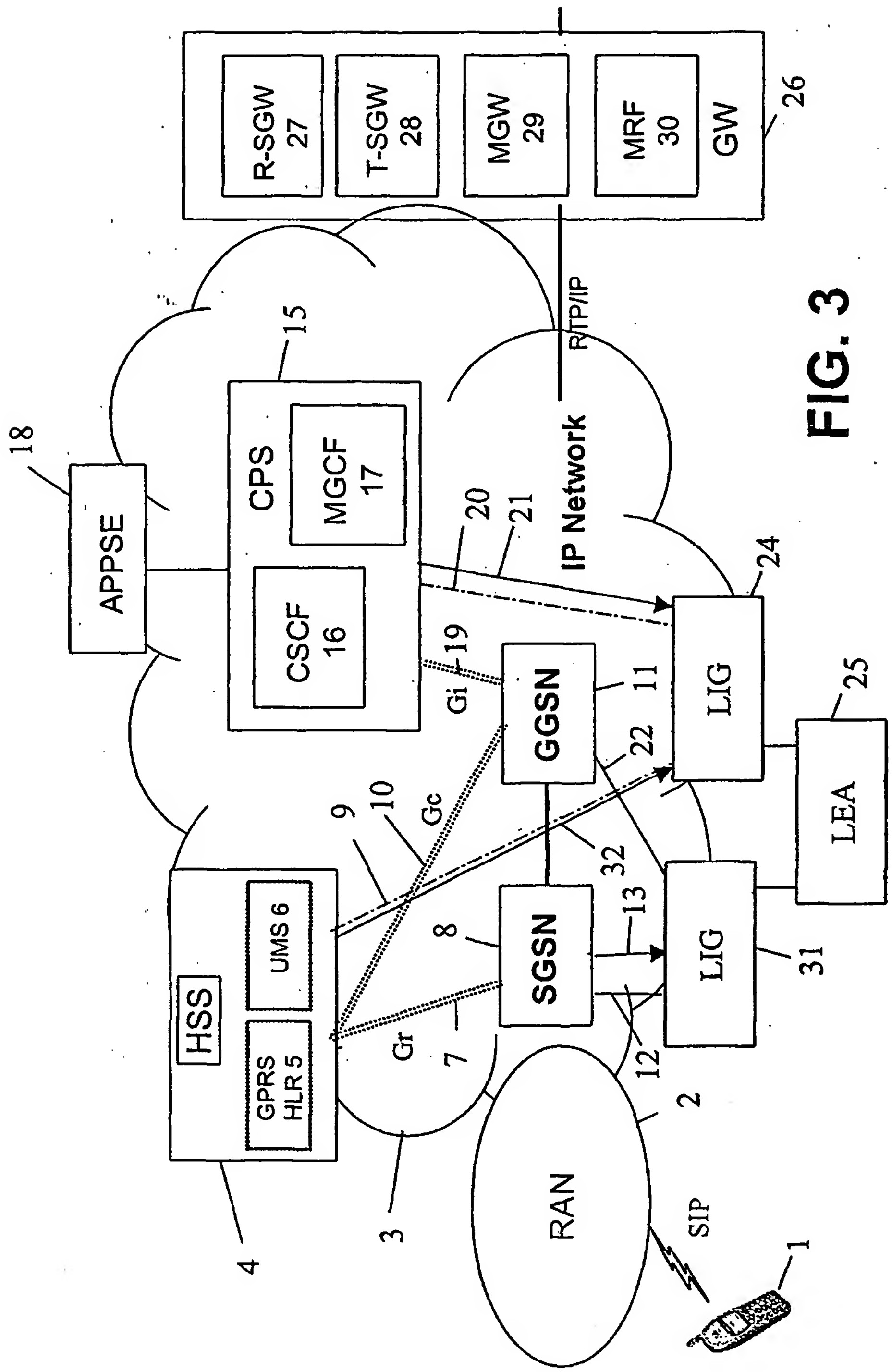

R-SGW 27
T-SGW 28
MGW 29
MRF 30
GW
26
RTP/IP
15
CPS
MGCF 17
CSCF 16
18
APPSE
20
21
IP Network
24
LIG
19
Gi
GGSN
11
22
25
LEA
9
10
Gc
32
HSS
UMS 6
GPRS HLR 5
8
SGSN
13
LIG
31
Gr
7
12
2
4
3
RAN
SIP
1

FIG. 3

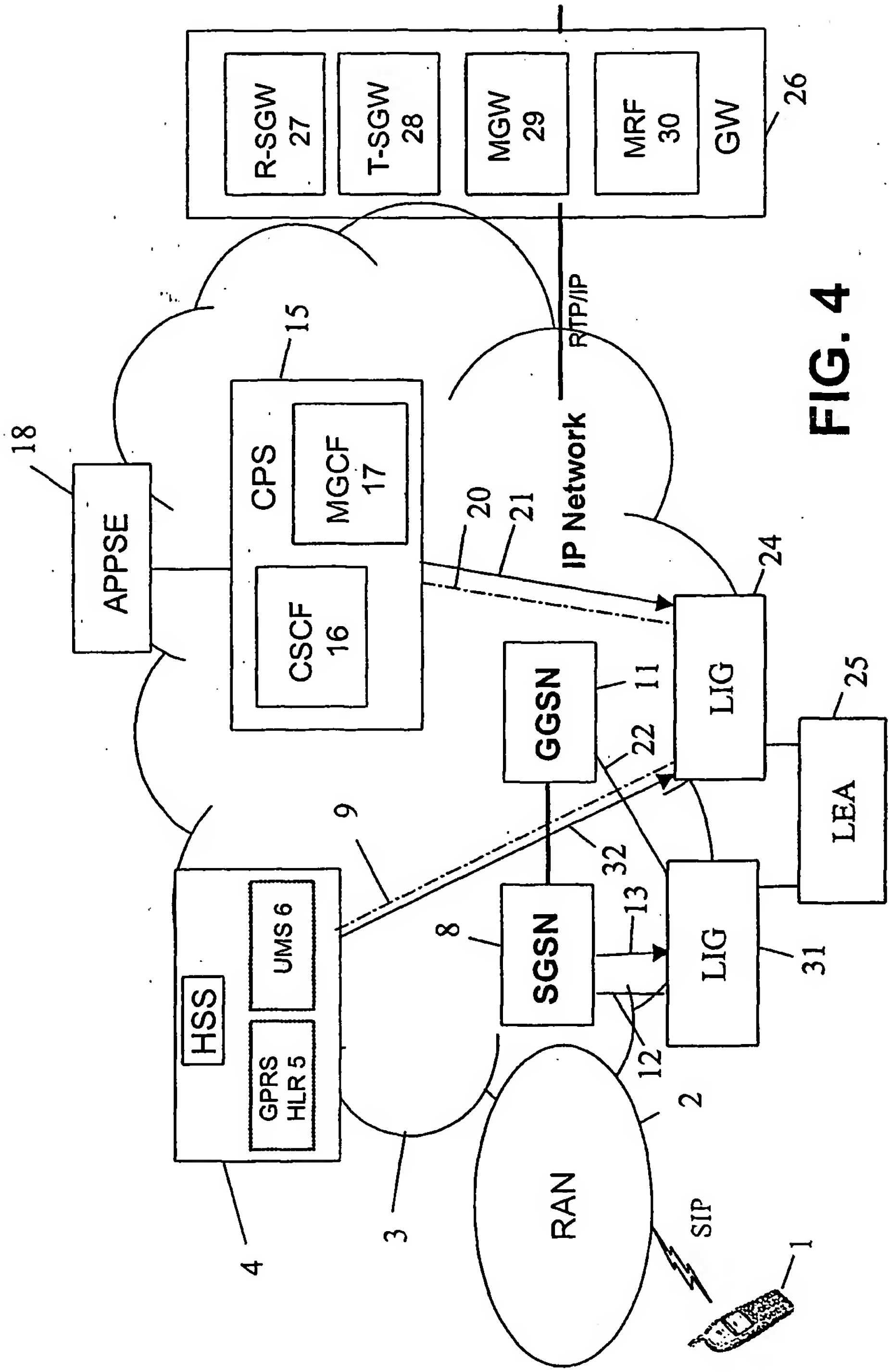

R-SGW
27
T-SGW
28
MGW
29
MRF
30
GW
26
RTP/IP
15
CPS
MGCF
17
18
APPSE
CSCF
16
20
21
IP Network
24
LIG
GGSN
11
22
25
LEA
9
32
HSS
GPRS
HLR 5
UMS 6
8
SGSN
13
LIG
31
12
2
RAN
SIP
3
4
1

FIG. 4

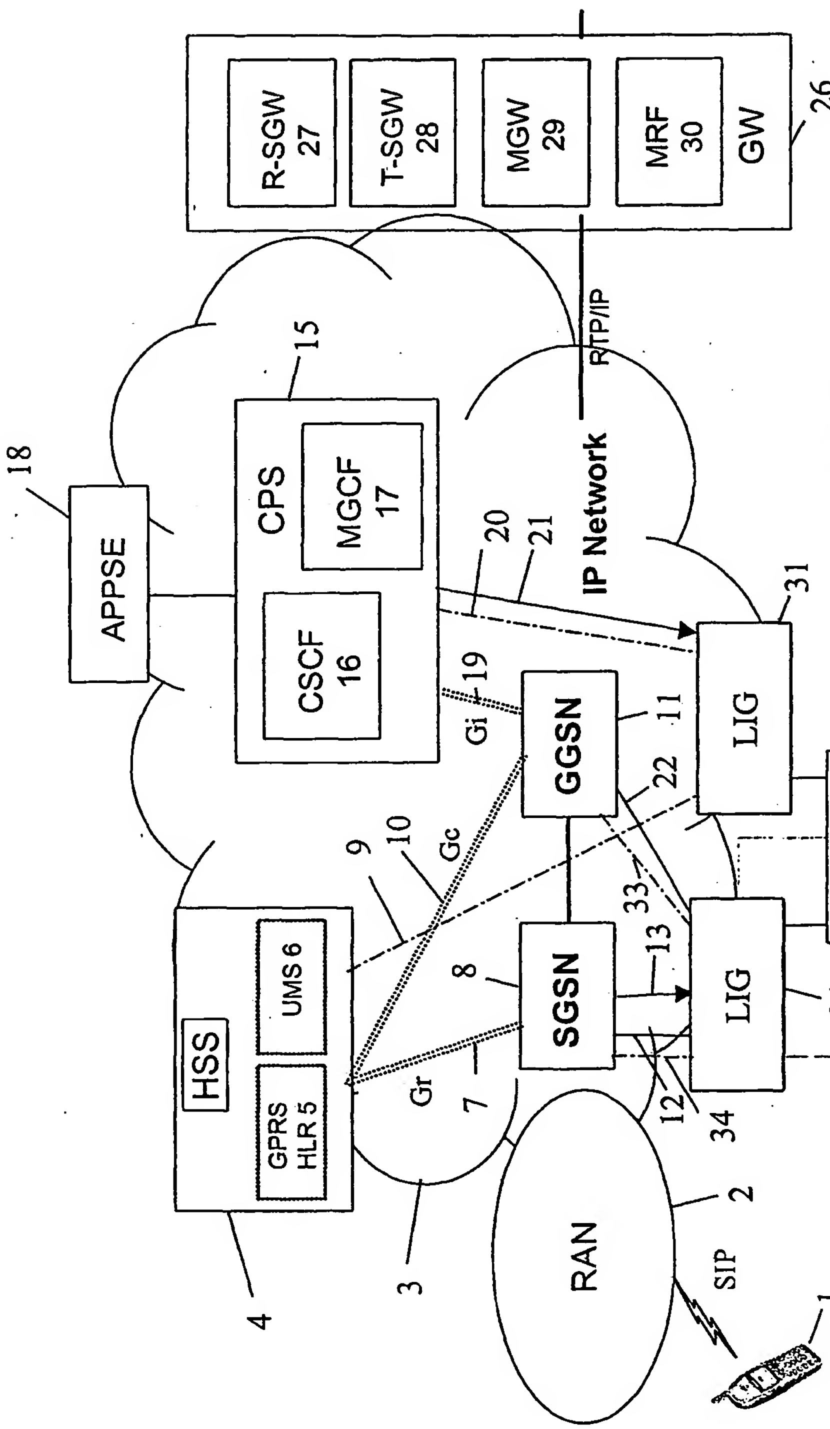

R-SGW 27
T-SGW 28
MGW 29
MRF 30
GW
26
RTP/IP
15
CPS
MGCF 17
CSCF 16
18
APPSE
IP Network
20
21
31
19
Gi
GGSN
11
LIG
25
LEA
22
33
9
10
Gc
HSS
UMS 6
GPRS HLR 5
8
SGSN
13
LIG
24
Gr
7
12
34
RAN
2
SIP
1
3
4

FIG. 5

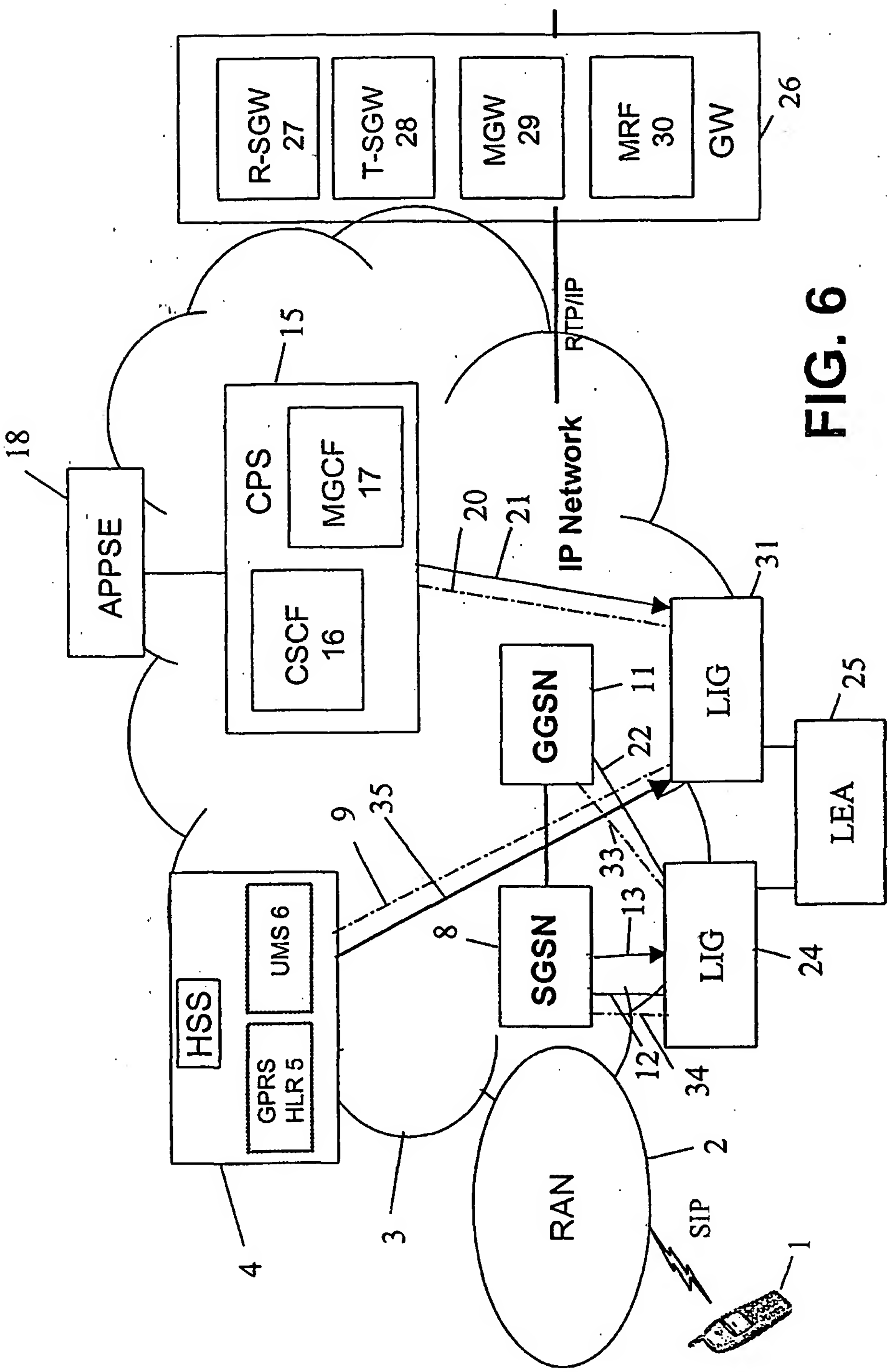

R-SGW 27
T-SGW 28
MGW 29
MRF 30
GW
26
RTP/IP
15
CPS
MGCF 17
CSCF 16
18
APPSE
IP Network
20
21
31
LIG
GGSN
11
22
LEA
25
HSS
GPRS HLR 5
UMS 6
9
35
33
13
8
SGSN
LIG
24
12
34
RAN
2
SIP
1
3
4

FIG. 6

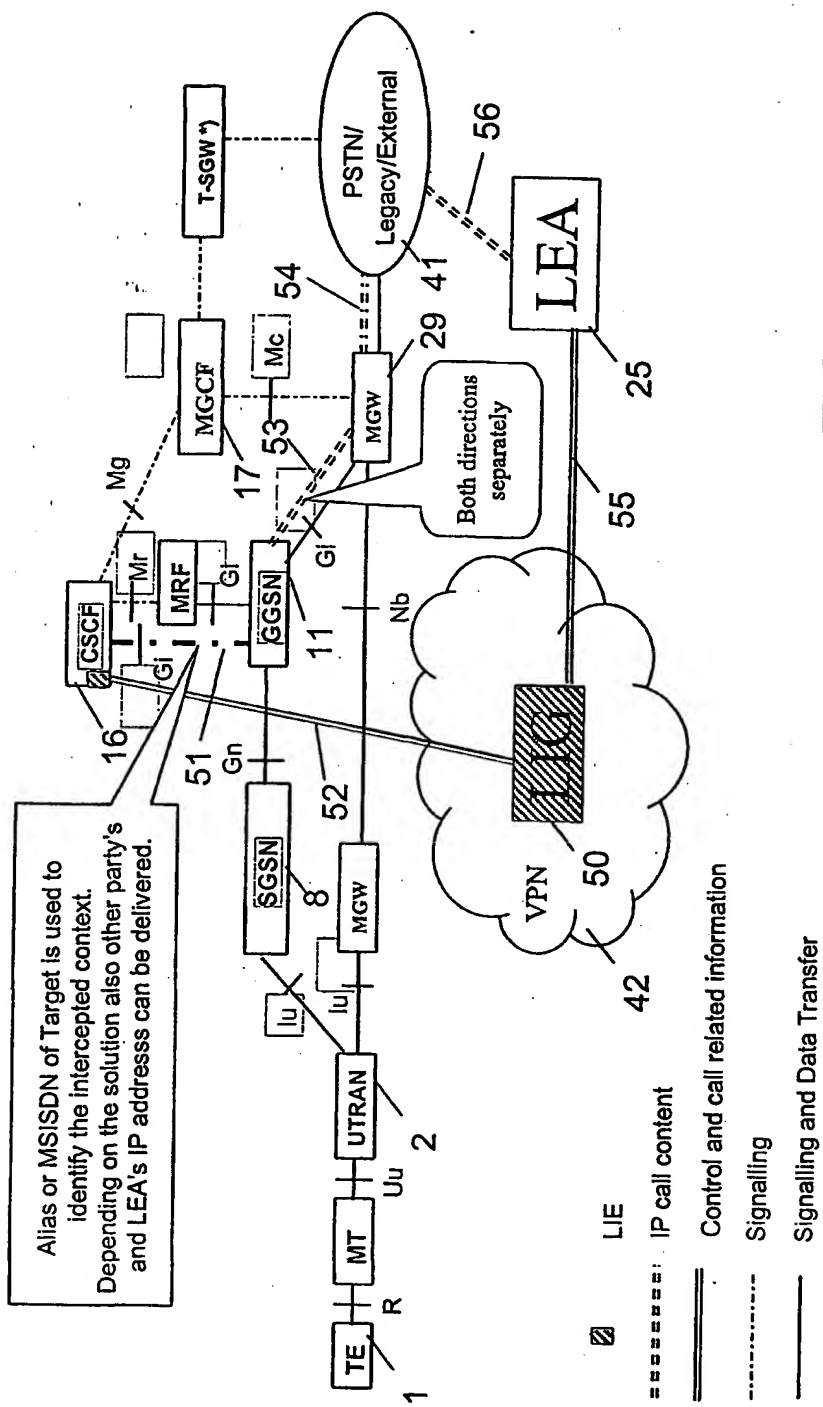

TE
R
MT
Uu
UTRAN
Iu
Iu
SGSN
MGW
Gn
GGSN
Gi
Gi
CSCF
MRF
Mr
Gr
Mg
MGCF
Mc
MGW
T-SGW *)
PSTN/ Legacy/External
LEA
LIG
VPN
Nb
Both directions separately
Alias or MSISDN of Target is used to identify the intercepted context. Depending on the solution also other party's and LEA's IP addresss can be delivered.
1
2
8
11
16
17
25
29
41
42
50
51
52
53
54
55
56
LIE
IP call content
Control and call related information
Signalling
Signalling and Data Transfer

FIG. 7

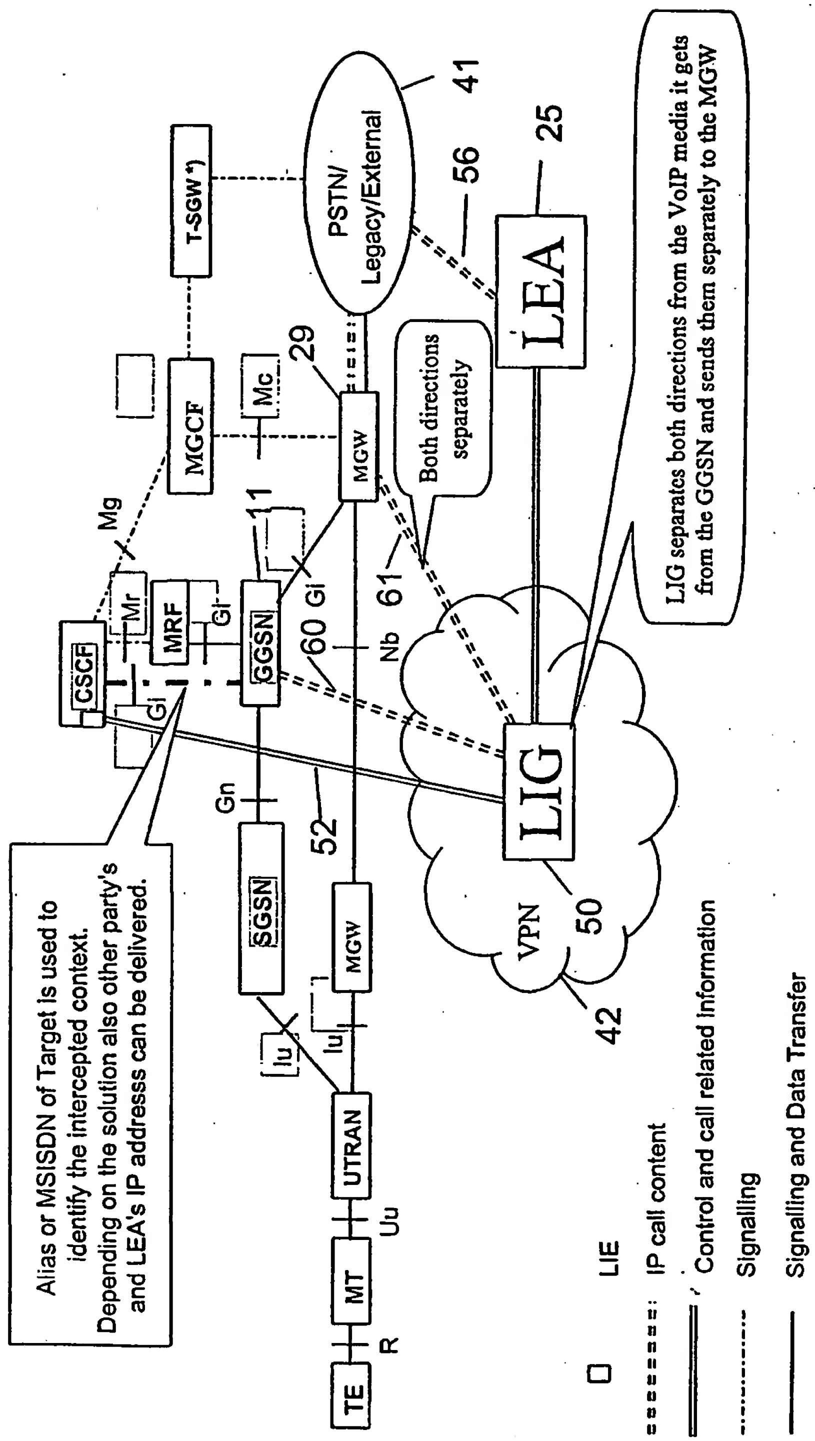

Alias or MSISDN of Target is used to identify the intercepted context. Depending on the solution also other party's and LEA's IP addresss can be delivered.
CSCF
Gi
Mr
MRF
Gi
Mg
MGCF
T-SGW *)
Mc
GGSN
60 Gi
11
Nb
61
MGW
29
PSTN/ Legacy/External
41
56
25
LEA
Both directions separately
LIG separates both directions from the VoIP media it gets from the GGSN and sends them separately to the MGW
Gn
52
SGSN
MGW
Iu
Iu
UTRAN
Uu
MT
R
TE
LIG
VPN
50
42
LIE
IP call content
Control and call related information
Signalling
Signalling and Data Transfer

FIG. 8

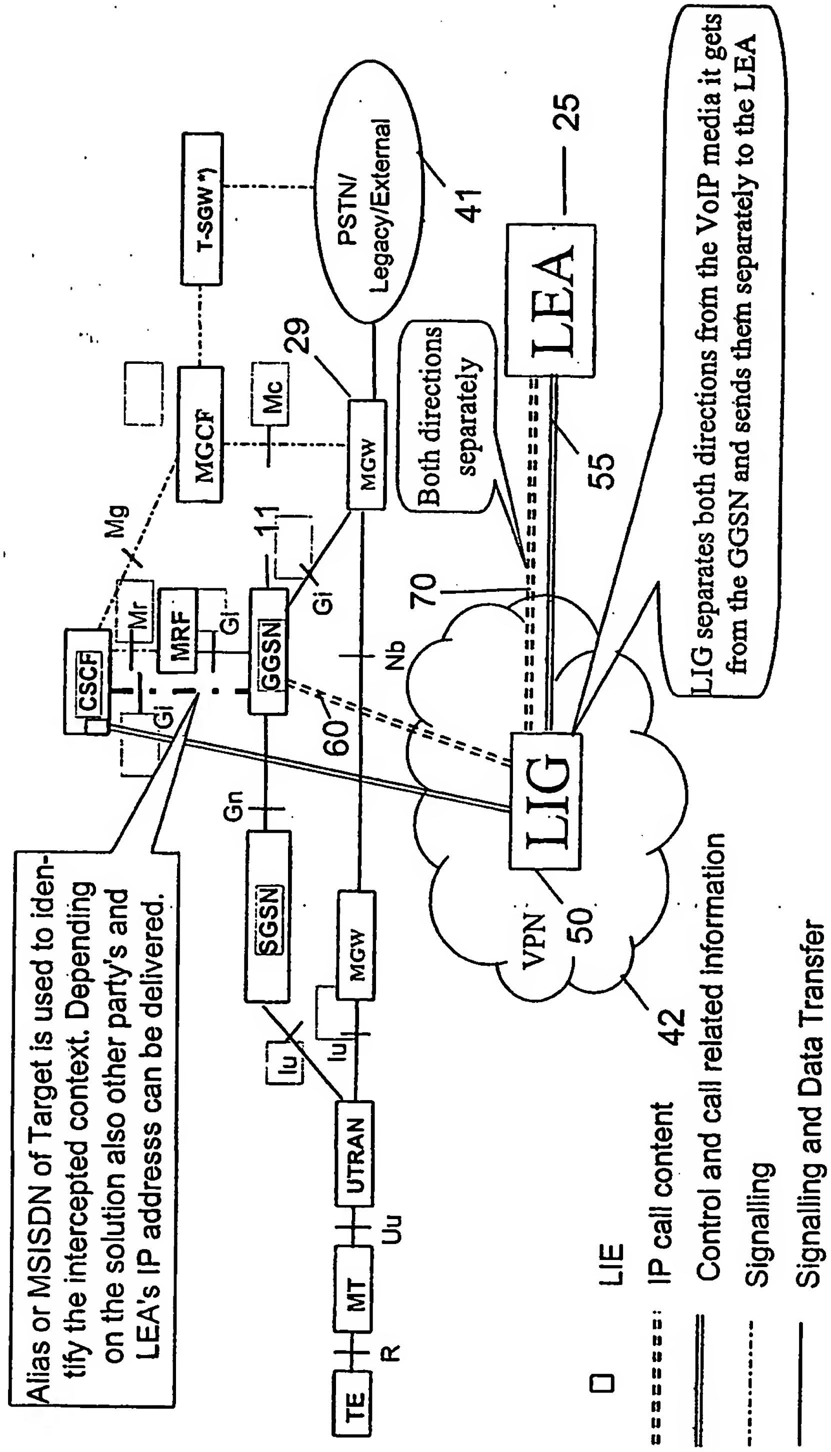

Alias or MSISDN of Target is used to identify the intercepted context. Depending on the solution also other party's and LEA's IP addresss can be delivered.
TE
R
MT
Uu
UTRAN
Iu
Iu
MGW
SGSN
Gn
GGSN
Gi
MRF
Mr
Gi
CSCF
Mg
MGCF
T-SGW*)
Mc
MGW
29
PSTN/
Legacy/External
41
11
Gi
Nb
60
70
Both directions separately
LEA
25
55
LIG
VPN
50
42
LIG separates both directions from the VoIP media it gets from the GGSN and sends them separately to the LEA
LIE
IP call content
Control and call related information
Signalling
Signalling and Data Transfer

FIG. 9

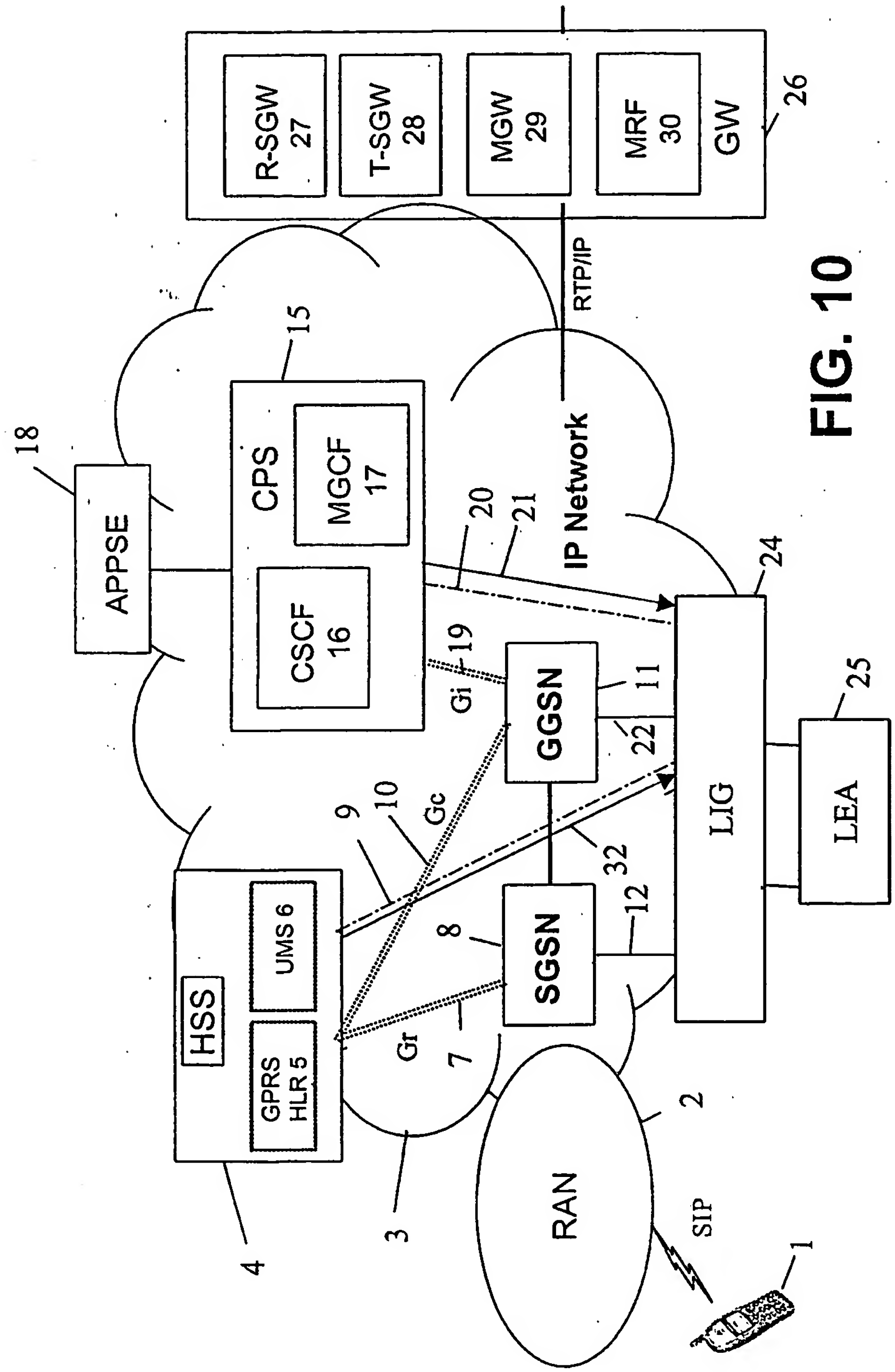

R-SGW 27
T-SGW 28
MGW 29
MRF 30
GW
26
RTP/IP
15
CPS
MGCF 17
18
APPSE
CSCF 16
20
21
IP Network
24
19
Gi
GGSN
11
22
LIG
25
LEA
9
10
Gc
32
HSS
UMS 6
GPRS HLR 5
8
SGSN
12
Gr
7
2
RAN
SIP
1
3
4

FIG. 10

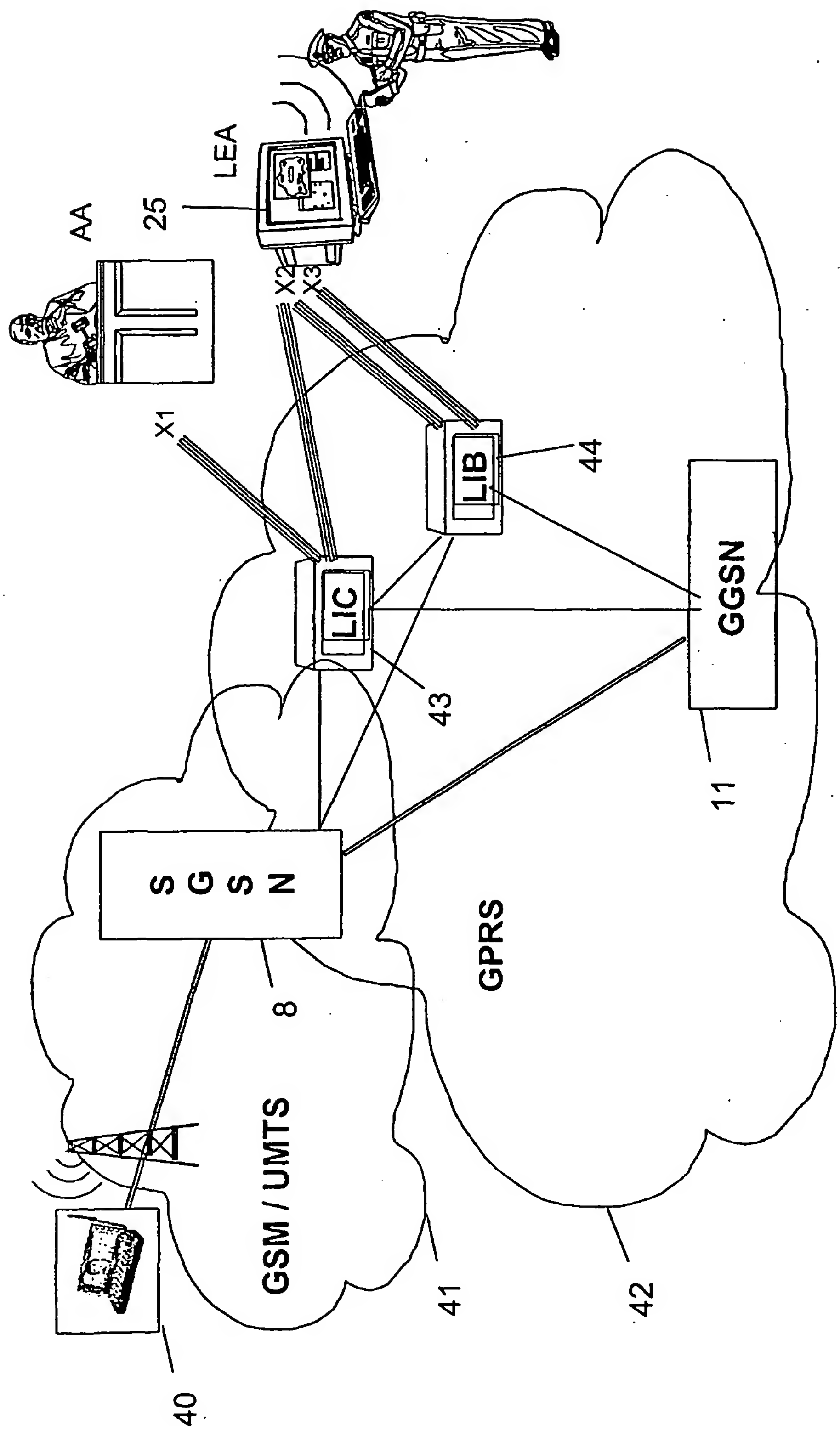

AA
LEA
25
X1
X2
X3
LIB
44
LIC
43
GGSN
11
SGSN
8
GPRS
GSM / UMTS
41
42
40

FIG. 11

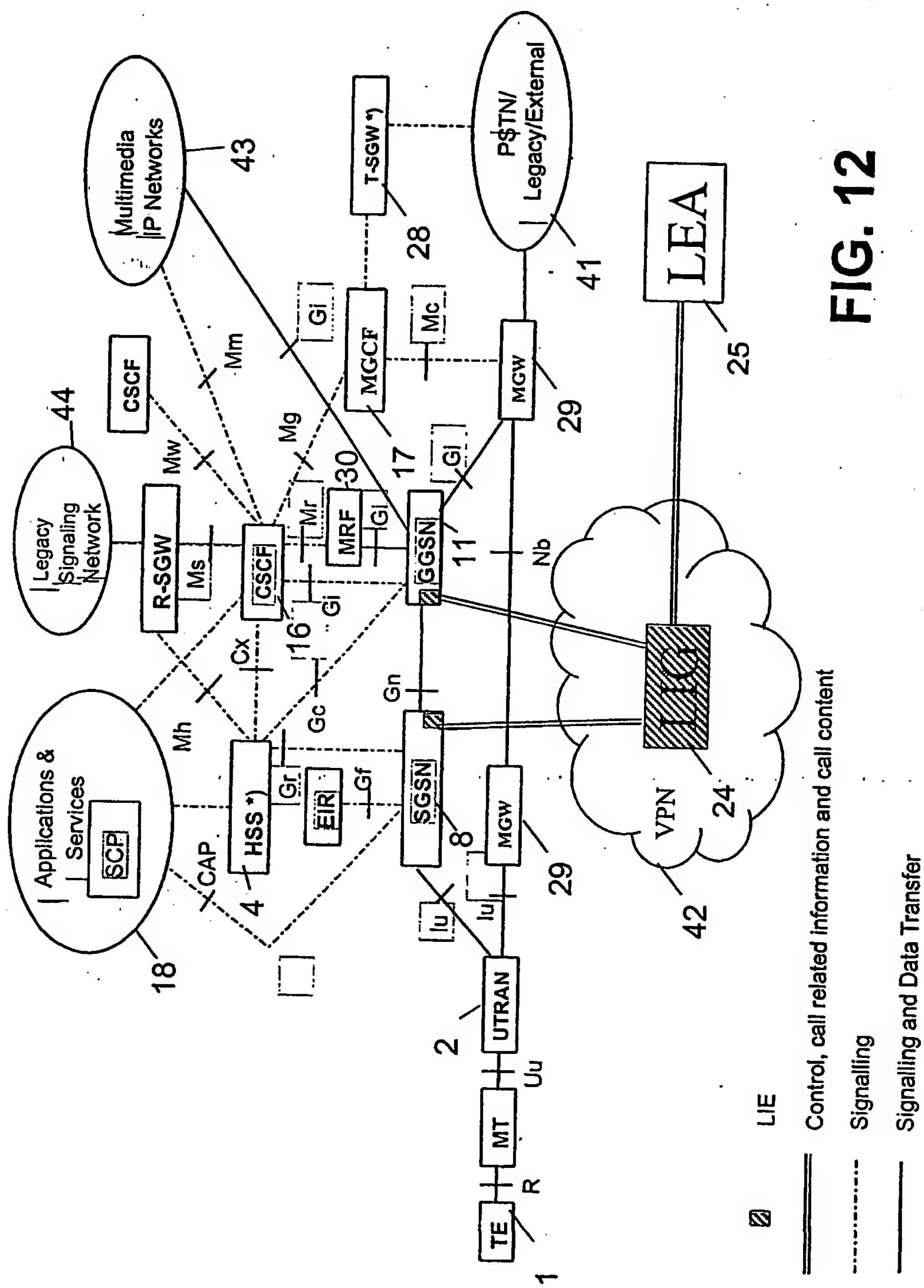

TE
MT
UTRAN
R
Uu
1
2
Iu
SGSN
GGSN
MGW
HSS *)
EIR
Gr
Gf
Gc
Gn
Gi
Cx
CAP
Mh
Mw
Mm
Mg
Mr
Ms
Mc
Nb
CSCF
MRF
MGCF
R-SGW
T-SGW *)
Applications & Services
SCP
Legacy Signaling Network
Multimedia IP Networks
PSTN/ Legacy/External
VPN
LIG
LEA
4
8
11
16
17
18
24
25
28
29
30
41
42
43
44
LIE
Control, call related information and call content
Signalling
Signalling and Data Transfer

FIG. 12

INTERNATIONAL SEARCH REPORT

onal Application No
EP 01/05583

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L12/26 H04L12/56 H04M3/22

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L H04M H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 00 42742 A (NOKIA NETWORKS OY ;HIPPELAEINEN LASSI (FI)) 20 July 2000 (2000-07-20) page 2, line 18 - line 31 page 3, line 15 - line 26 page 4, line 7 -page 5, line 14 page 5, line 32 -page 6, line 2 page 6, line 26 -page 7, line 7 page 8, line 10 - line 26 page 17, line 22 - line 24 abstract; figures 1-3 ---	1-44
A	WO 99 55062 A (GTE GOVERNMENT SYST) 28 October 1999 (1999-10-28) column 2, line 34 -column 4, line 14 column 5, line 16 -column 6, line 46 abstract ---	1-44

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
15 January 2002	06. 02. 2002

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Elisabet Aselius

INTERNATIONAL SEARCH REPORT

I ional Application No
/EP 01/05583

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	STEPHEN P SMITH ET AL: "Independent review of the carnivore system." IIT RESAERCH INSTITUTE, DRAFT REPORT, 17 November 2000 (2000-11-17), XP002902233 Contract No. 00-C-0328 IITRI CR-022-216 section 3, 4-3, 5,5 ---	1-44
E	WO 01 89145 A (ERICSSON TELEFON AB L M) 22 November 2001 (2001-11-22) page 2, line 1 -page 4, line 2 claims 1-18; figures 1-6 ---	1-44
A	US 5 913 161 A (OZULKULU E ET AL) 15 June 1999 (1999-06-15) abstract -----	1-44

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
EP 01/05583

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
WO 0042742	A	20-07-2000	WO	0042742 A1	20-07-2000
			AU	2617399 A	01-08-2000
			EP	1142218 A1	10-10-2001
WO 9955062	A	28-10-1999	AU	3865599 A	08-11-1999
			WO	9955062 A1	28-10-1999
WO 0189145	A	22-11-2001	WO	0189145 A2	22-11-2001
US 5913161	A	15-06-1999	NONE		